The NIH Eye on Privacy

Office of the Senior Official for Privacy | Volume 2, Issue 2 | May 2009

The Office of the Senior Official for Privacy serves as the chief NIH privacy governance entity whose mission is to ensure the highest level of scientific integrity, public accountability, and social responsibility in the area of privacy management.

Web 2.0 Technology is Ready. Are We?

Web 2.0, social media, and new media refer to technology that combines online communities, extreme interactivity and collaboration. Where Web 1.0 (e.g., e-mail, Web sites, and search engines) connects people to information, Web 2.0 (e.g., podcasts, blogs, RSS feeds, and social networking) connects people to other people.

On March 26, President Obama held an online town hall meeting that drew almost 100,000 participants

Social media is on the government's radar. In the first days of his administration, President Obama issued a FOIA mandate for more transparency across Federal agencies, in part through the use of new technologies. While Government agencies have not embraced social media as quickly as the private sector, the interest is definitely on the rise.

NIH is working to consider the security risks of adopting social media on a broader basis. Dan Sands, Chief Information Security Officer for NIH, states in the January 23 issue of the *NIH Record,* "These [Web 2.0] applications can introduce new risks into the enterprise that need to be assessed and mitigated. It's the security community's unenviable job to prevent undue risk to the IT resources we depend on to support the NIH mission and to prevent the compromise or loss of the research, scientific, patient or personal data entrusted to us."

The Department's Web Content Team believes social media will become increasingly relevant as the workforce includes more people who are accustomed to using social media in their personal lives. To exchange ideas on this hot topic and offer you a voice in the discussion, they have created a new media Web site (http://www.newmedia.hhs.gov) as well as a listserv (List HHS-NEWMEDIA).

Subscribe to the HHS New Media Listserv

1. Visit https://list.nih.gov
2. Search "HHS-NEWMEDIA"
3. Select list and click to join!

While we wait for further evaluation of Web 2.0 technologies and HHS guidance, we encourage you to join the discussion!

Karen Plá
NIH Senior Official for Privacy

Egregious Violations, Serious Consequences, and Maybe a New PR Firm!

The Incident: Largest Data Breach Ever

The Accused: Heartland Payment Systems (Princeton, N.J.), which processes payroll and credit card payments (100 million transactions per month)

Media Coverage in the Past Month: 233 hits on GoogleNews

Timeline of Events:

Fall 2008

- Malicious software compromises the company's network, exposing consumer credit card data
- Heartland is alerted to suspicious activity by Visa and MasterCard and hires forensic auditors

January 2009

- Heartland announces the data breach some experts call "the largest ever"
- Heartland claims no merchant data, SSNs, unencrypted PINs, addresses, or telephone numbers were exposed
- Heartland launches a breach Web site to provide information to customers, who are not liable for fraudulent charges
- A lawsuit, filed in U.S. District Court in Trenton, N.J., alleges Heartland failed to: protect consumer data, notify consumers about the incident in a timely manner, and compensate affected consumers for costs associated with identity protection

March 2009

- Congress holds a hearing to question whether the Payment Card Industry Data Security Standards, created and regulated by credit card companies, sufficiently protect information
- Retail representatives claim the self-regulatory system sacrifices some consumer protections for the sake of conveniencing credit card companies
- Credit card industry maintains self-regulation is effective, pointing out that since standards were published, security breaches only occurred due to non-compliance

This is another incident to remind us how important it is to safeguard personal information!

Web 2.0 and Government in the News

"Twitter: Under Attack"—*Tech Republic*
http://blogs.techrepublic.com.com/security/?p=1402&tag=nl.e036

"GSA signs an agreement with Facebook"—*Federal Computer Weekly*
http://fcw.com/articles/2009/04/10/web-facebook-gsa.aspx

"Who's Tweeting in Government?"—*Government Computer News*
http://gcn.com/blogs/tech-blog/2009/04/government-tweets.aspx

To meet federal requirements, NIH has created its own social media channels:

http://www.youtube.com/user/nihod
http://www.twitter.com/NIHforFunding
http://www.twitter.com/NIHforHealth

YouTube Broadcast Yourself™ twitter

NIH has also established policy for Peer-to-Peer software:

P2P Policy—http://ocio.nih.gov/security/NIH_P2P_Policy.doc

P2P Guide—http://ocio.nih.gov/security/NIH_P2P_File_Sharing_Guide.doc

We recommend you use Adobe Reader 9 to view this document. If you experience any technical issues, please contact your IT group.
For more information about the OSOP, the Privacy Act, PIAs and privacy at NIH, please visit: http://oma.od.nih.gov/ms/privacy
To learn more about IT security at NIH, please visit: http://ocio.nih.gov

Q: Why do we need the Privacy Act and what does it do?

A: As Americans, we have a constitutional right to privacy. The Fourth Amendment of the U.S. Constitution promises the right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This right includes protecting the privacy of individuals' personal information which the Federal government collects, maintains, uses and disseminates.

In general, the Privacy Act of 1974, as amended, prohibits unauthorized disclosures of personal information. In part, the Act provides, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." Pursuant to the Privacy Act, Federal agencies must implement safeguards to protect the security and accuracy of information within its purview. As U.S. citizens or resident aliens, the Privacy Act affords us the right to access and correct records the government maintains on us, unless the records fall within one of the exceptions or exemptions articulated in the Act.

To learn more about privacy, read our FAQs.

Meet Your Privacy Coordinator:
Jerry King

Jerry is the CC Privacy Officer. He has worked at NIH for 30 years and plans to retire this year. Jerry previously served as the Assistant Director and Director of the Medical Record Department. He currently serves as the DCRI Senior Program Manager and is busy training Sue Martin to step into his privacy role. Jerry can be reached at jking@cc.nih.gov and Sue can be reached at smartin@cc.nih.gov.

Jerry's best piece of advice:

Remember that all PII should be treated with the utmost care—whether it pertains to employees, patients or the public.

Jerry's thoughts on privacy:

"Individuals participate as research subjects at NIH on a completely voluntary basis. If we, in our role as privacy professionals, cannot maintain their privacy and the confidentiality of the sensitive information about them that is collected, then the entire mission of the NIH could be negatively affected if their continued participation in research were to be jeopardized."

Privacy Rules Hamper Adoption of Electronic Medical Records, Study Says

By Jaikumar Vijayan, *Computerworld,* April 14, 2009

In a study that is unlikely to find favor among privacy advocates, researchers warn that increased efforts to protect the privacy of health data will hamper the adoption of electronic medical records (EMR) systems. The study, conducted by researchers at MIT and the University of Virginia, said EMR adoption is often slowest in states with strong regulations for safeguarding the privacy of medical records.

On average, the number of hospitals deploying EMR systems was up to 30% lower in states where health care providers are forced to comply with strong privacy laws than it was in states with less stringent privacy requirements. The study found privacy rules often make it harder and more expensive for hospitals to exchange and transfer patient information, thereby reducing the value of an EMR system.

Read the full story: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131578

GAO Report Update

Freedom of Information Act (FOIA)—
DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness.
http://www.gao.gov/new.items/d09260.pdf

National Cybersecurity Strategy—
Key Improvements Are Needed to Strengthen the Nation's Posture.
http://www.gao.gov/new.items/d09432t.pdf

Information Technology—
Challenges Remain for VA's Sharing of Electronic Health Records with DOD.
http://www.gao.gov/new.items/d09427t.pdf

Calendar of Events

International Association of Privacy Professionals (IAPP)

CIPP Foundation & CIPP/G Certification Testing
May 6, 3–7 p.m., Ernst & Young
621 East Pratt Street, 5th floor, Baltimore, MD

American Society of Access Professionals (ASAP)

ASAP Training Series
May 12–14, Washington, DC
GWU Marvin Center

EPA Web Training: Earth Month Outreach

Mixing Web 1.0 and 2.0
May 20, 1–2 p.m.

Web 2.0 offers new, exciting ways to engage the public. But the first step is to consider why a certain Web 2.0 tool should be used, rather than the perceived need to use a Web 2.0 tool. This training will review EPA's 2008 Earth Day month suite of Web 2.0 tools as a part of an overall communications strategy to spark interest and lead people to the EPA's Web site.

Register here:
https://www1.gotomeeting.com/register/237080329

Privacy Coordinator Group Meeting

May 27, 9:30–11:30 a.m.
6130 Executive Blvd. (EPN), Conference Room G

DHS Gov 2.0: Privacy & Best Practices Workshop

June 22–23, Washington, DC
Washington Court Hotel

The DHS Privacy Office is holding a public workshop to bring together leading academic, private sector, and public sector experts to discuss the privacy issues posed by Government use of social media.

To register, call (703) 235-0780 or e-mail privacyworkshop@dhs.gov with "Government 2.0 Workshop" as the subject line and with your name and organization in the e-mail.

Receive the NIH Eye on Privacy directly to your e-mail inbox!
To subscribe, please visit: http://oma.od.nih.gov/ms/privacy/niheyeonprivacy.html

NIH Office of Management Assessment
6011 Executive Blvd., Suite 601 | Phone: (301) 451-3426 | Fax: (301) 402-0169 | privacy@mail.nih.gov

U.S. Department of Health and Human Services
National Institutes of Health

We recommend you use Adobe Reader 9 to view this document. If you experience any technical issues, please contact your IT group.
For more information about the OSOP, the Privacy Act, PIAs and privacy at NIH, please visit: http://oma.od.nih.gov/ms/privacy
To learn more about IT security at NIH, please visit: http://ocio.nih.gov